A Very Simple User Access Control Technique through Smart Device Authentication using Bluetooth Communication

Sohum Misra
Applied Electronics and Instrumentation Engineering, Heritage Institute of Technology
Chowbaga Road, Anandapur, Kolkata -700107
Email: (misra.sohum@gmail.com)

Abstract

Large scale adoption of smart devices like smart mobile phones for personal usage has opened up an opportunity to identify individuals via their smart device identities. This paper aims to achieve very simple technique of users' access control through device authentication using a microcontroller board such as Arduino that interacts with the smart device using Bluetooth technology which is almost available in every smart device. The implementation procedure is discussed through the experimentation. As a methodology of secured communication, password protection is used in the mobile apps. Some possible application areas are discussed in which the proposed methodology may be applied to enable appropriate services. The novelty of this work is to provide a simple and low cost solution for users' access in a secured protected place. Further, the proposed authentication mechanisms are intuitive and require minimum effort.

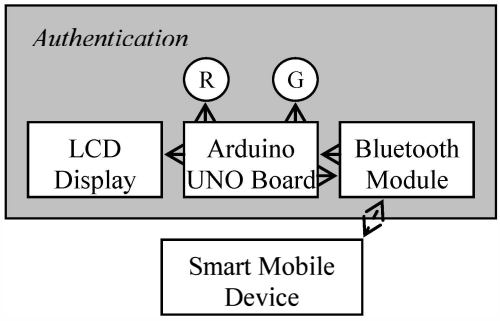
I. Introduction

Access control is basically identifying a person for giving entry or access authenticating him by looking at his identification, then giving that person only the key to the door. The percentage of population using smart mobile devices is increasing at a rapid rate [1]. This has opened up opportunity of associating a device identity with an individual and using this device identity as an alternate identity that may be used in secured premises for restricted users' entry or the places valid only for registered/authorized users. These places may be libraries, museum, research laboratories, gold shop, defense areas or even within a private home etc. Robust device identification may be used as a solution strategy.

As scenario descriptions consider a scientific research laboratory which has only access to limited researcher and some authorized persons. In most places **Touch keypad** [2] with graphical display may be used where users are entitled to put their signature in the form of password / PIN for the access. There is every possibility of peering over the shoulder to know the PIN. Direct contact or presence of man-in-the middle can make the security of a place or system vulnerable. In many places **personal card or identity instrument in the form of smart device** is also provided. Installing security system components outside the organization may always have chances of tampering.

There are number of ways [3,4,5] access control can be achieved in terms of smart device authentication and one of the secured ways is to take advantage of the wireless communication between the device and the authentication platform to perform the identification. The wireless communication technology would determine the range of proximity to conduct the authentication [6]. But Wireless transmission always contains some degree of threat to outsider attackers such as man-in- the middle attack.

In this paper, we propose a solution methodology that is low cost and simple and eliminates the above problems. This procedure needs only to carry the user's smart mobile phone that has Bluetooth communication facility and a low cost Microcontroller device such as Arduino board. Fig. 1 shows the block diagram of the model.



Legend: R: Red LED, G: Green LED

Figure 1: Block Diagram

The Arduino micro-controller board is used here as the main base to create the platform to establish link with the smart device and carry out an encrypted communication. It can be coded in high-level (java like) language. As this is a concept project, the board is used here to simply demonstrate the process of communication.

We are looking at performing the authentication within 10 meters. This would enable securely keeping the authentication platform distant from the device it authenticates, yet not so far that large number of devices is within its communication range. Hence, Bluetooth [7] qualifies for the desired range of 10 meters. Moreover, most of the smart devices have inbuilt Bluetooth communication option that can be

used for this solution without adding extra hardware and complexity for the design.

Therefore, this short paper work use a well known low cost Arduino UNO board [8] along with relevant components to implement the authentication platform. This assumes that a mobile app would be installed in the mobile smart device which would be able to communicate the device identity over Bluetooth protocol to the authentication platform. The authentication platform would then conduct the verification process and indicate the result appropriately.

The rest of the paper is organized as follows. Section II describes the possible vulnerabilities and remedies. Section III is the design methodology, Section IV is the implementation strategy, Section V is the test results and discussions. Finally, section VI provides the conclusion.

II. Vulnerabilities and Remedies

The proposed system demands low energy requirement, is affordable, reliable and portable. Thus, it is ideal for wide range of applications. It can be used in libraries for specific customers or for selective access, in corporate branches as an alternative for cards, for military access or restricted areas where entry/access-permit is a must.

The proposed system enables authentication of a personal device by another device in a contact-less manner. This system would be useful for implementing access control. In this case, the personal device would typically be the smart phone of the person who wants to get access and the other device which verifies the identity would be owned by the organization that is enforcing the access control.

The following list provides the vulnerabilities and suitable remedies:

1. Theft of the personal device: The identity is transmitted from the mobile phone using a mobile application. This application is password protected. In the event the mobile phone is stolen, the mobile application that transmits the identity cannot be invoked. Most of the smart phones have feature of password so the phone itself would not be usable without the phone password. This adds 2 layers of security at the personal device level.

2. Man-in-the-middle Attack: The mobile application and the other device that verifies the identity would incorporate strong encryption techniques to obviate any man-in-the-middle attack.

3. Peering over the shoulder: As the smart phone never leaves the possession of the person seeking access, any PIN he provides would not be easy for someone else to view and know.

4. Limiting features of mobile: To preserve security of a protected area many times organizations need to disallow usage of smart phones within the area. However, with the above mechanism the mobile app that is loaded for identity verification can well be used to disable certain features of the smart phone, like camera, message, calls, etc. To ensure that the app is live for the duration of the stay, the app can be programmed to send heart-beat signals to the verification device. *This idea is very novel in the sense that without depositing the costly smart personal device with the organization authority, essential security can be enforced at the same time eliminating users' worries of misplacement of the personal device.*

5. Not carrying the identity instrument: It is highly unlikely that person would step out without his mobile phone nowadays. This reduces the chance of showing up at the access control point without valid identity provided the entire access control is invoked through the mobile phone app.

III. Design Methodology

The design methodology is divided into two units:

The Arduino Unit: The heart of the authentication platform uses Arduino UNO as the microcontroller which orchestrates the process of reading the input transmitted by the smart mobile device, comparing the information with the database, and sending output to the LEDs and LCD panels for human interfacing. It also sends the result to the **mobile app** running on the smart mobile device.

The Mobile App: The mobile app reads the device identity (like IMEI number of mobile phone), converts that into a string and communicates the same to the authentication platform. For security reasons the mobile app is **password protected**. For this experiment an Android mobile phone has been used as the smart mobile device.

IV. Design Implementation

The following are the required components for implementing the project:

1. Arduino (UNO) board
2. Bread board
3. Bluetooth module compatible with Arduino (linvor-JY-MCU)
4. LCD Display
5. LEDs
6. Power supply (5 V, 0.5 A)
7. Application in the mobile phone for serial Bluetooth communication
8. Connecting wires

Arduino Unit:

To create the hub, an Arduino UNO board is used (Fig. 1) connecting to a bread board. Two LEDs, red and green, are used as feedback signals after checking for authentication. A Bluetooth module (linvor [9]) is used which serves as the signal receiver at the hub end. The functions of the different components are discussed below.

- **Arduino UNO:** The Arduino UNO is a high level microcontroller board. It is based on the ATmega328 microcontroller IC chip [10]. It has 14 digital input/output pins, 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. The Arduino UNO board is a basic board containing aids to meet the basic requirements of a microcontroller. It is connect to a computer with a USB cable or powered with an AC-to-DC adapter or battery to get started.
- **LEDs:** Two LEDs are connected to two digital pins of the Arduino board and the other ends of the LEDs are grounded. The microcontroller is so programmed that the Red LED will glow by default. If a device being checked is authentic, i.e. registered, the green LED will glow for some time indicating the authenticity of the device. In any other case, the Red LED will continue to glow. No external resistors are required as the digital pins of Arduino board contain internal pull-up resistors.
- **Bluetooth Module:** The Bluetooth module contains 4-pins generally. Two pins are used to provide power to the device, hence are connected to V_{cc} and ground. The other two pins are used for transmission and reception of serial data. The "TX" (transmission) pin of the Bluetooth module is connected to a digital pin of microcontroller used for receiving the data and the "RX" (reception) pin of the Bluetooth module is connected to a digital pin of Arduino board used to transmit the data. This setup facilitates serial communication of data wirelessly. Bluetooth modules can communicate up to a range of 5m - 10m. The devices need not be present at Line of Sight. This serves to be an advantage.
- **LCD display:** A compatible LCD display is connected to the Arduino, to display some information. The LCD display requires a potentiometer to control the contrast of the display.

Mobile App Unit:

For this part, an Android application known as S2 Bluetooth is used. It is used to establish a serial communication [11] Bluetooth platform between the Arduino board and the mobile phone. In this work, a comma separated string is constructed and sent from the mobile app where the string before the first comma is the unique identification code (UIC) and the part following the comma is the information. Thus the format is: "<UIC>, <Information>"

The mobile app is password protected and will use the smart device's Bluetooth facility to detect the hub automatically and send the device ID for verification. For greater security, the string being sent can be encrypted [12]. The application can also be extended so that it can use other functions and sensors fitted in the smart device for various purposes.

The experimental implemented circuit is shown in Fig 2. The most attractive feature is that contact less communication is established with the authenticated system placed completely inside the organization security perimeter **eliminating the chances of external tampering of security devices.**

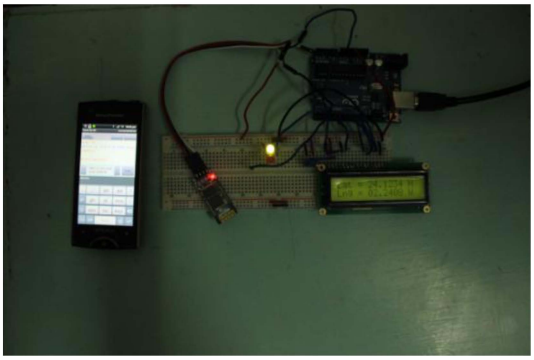


Figure 2: Working System

Following notes are very important for the design.

Notes

- The digital pins of the Arduino UNO board are used for interfacing with the LEDs. As these pins have internal resistances so **no external resistors are needed for digital pins reside in the board.**
- As we are using C++ like high level language to program the system, the **solution is easily maintainable.**
- The authentication platform runs **on low power** (5v, 0.5A) making it suitable **for long battery based usage.**

V. Testing and Result

Step 1: The S2 Bluetooth mobile app is invoked in the mobile phone running Android platform.

***Result*:**

- The mobile app opens on the mobile app. If the Bluetooth of the mobile phone is not on, the app would request to turn it on.

Step 2: The Arduino microcontroller board is powered on.

Step 3: The sketch (code written for the Arduino platform) is uploaded in the board. The sketch contains a set of UIC.

Step 4: The Bluetooth of the Arduino and that of the mobile phone is paired

***Result*:**

- The LCD display connected to the Arduino board initially displays a text "Working well".
- The Green LED is turned off and the Red LED is turned on
- The mobile app receives a text "power on".

Step 5: "<UIC>,<Information>" string is sent from the mobile app

***Result*:**

If the **UIC matches** with any one of the preloaded set of UIC that is a part of the sketch,

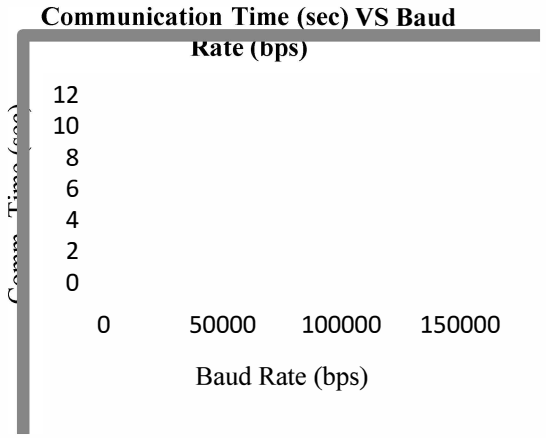
- The Green LED glows for 3 seconds and the Red LED is turned off for that period.

- Strings after the first comma, the information part, is displayed on the LCD display for 3 seconds.
- A text is displayed in the mobile app that reads **"Access Granted**..".
- After 3 seconds, the Red LED is turned on again and the Green LED is turned off.
- The word **"next…" is displayed** on the LCD display.

If the code **does not match**,

- A text is displayed in the mobile app that reads "**Didn't match, sorry access not granted".**

The time taken for transfer of information between smart phones/devices and Arduino is measured in Baud Rate. Baud Rate is defined as a data transmission rate measured in bits per second. In this project, the time taken (in seconds) for this communication varies with Baud Rate as:



From the graph, it can be understood that the time taken for information transfer is decreasing with increase in Baud rate, i.e., higher Baud rate is speeding up the whole process.

Discussions: Many organizations have security policies where no one is allowed to enter the security zone with smart phones. This is because these devices have inbuilt cameras, location and position detection sensors, internet connectivity and recording facilities which make these devices agents of information vulnerabilities. Hence, visitors to these places need to deposit their smart phones at the security desks. As people are not comfortable to leave their costly personal device with third party agencies, a very simple solution can be provided where an individual is allowed to carry their smart phone(s) with them, but a mobile app is installed and activated to limit the features of the phones as per security requirements. The mobile app needs to send heart-beat signals to a hub to ensure that the app is running during the stay. This mobile app can be used as an extension to the mobile app that allows device authentication to strengthen security process.

VI. Conclusion

In this paper, a very simple mechanism of users' access control via smart mobile device authentication is discussed. A model has been implemented using Bluetooth communication and Arduino microcontroller board. The important aspect of this work is the **concept of using smart phone** instead of electronic identity cards or other instruments as access control device, and smart phones are carried by every person nowadays. This is a low cost yet effective solution for access control.

This method may be extended to track visitors and authorized persons' movement within a campus such as university place, colleges, museum etc.

References

1. "The World in 2013: ICT Facts and Figures" Website: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf;
2. Honeywell, "Security System, User's Manual, 4110DL/4110XM, ADEMCO, September 1996", Website: http://www.security.honeywell.com/documents/4110DLUM.PDF.
3. "Improvements to NFC Mobile Transaction and Authentication Protocol" http://eprint.iacr.org/2013/035.pdf.
4. "Strong Authentication Using Smart Card Technology for Logical Access", Publication Date: November 2012. http://www.smartcardalliance.org/pages/publications-strong-authentication-using-smart-card-technology-for-logical-access.
5. "Security Token (Authentication Token)" http://searchsecurity.techtarget.com/definition/security-token.
6. "NFC Forum : FAQ", Website: http://www.nfc-forum.org/resources/faqs#howwork.
7. Jaap C. Haartsen, BLUETOOTH – The Universal Radio Interface for Ad Hoc, Wireless Connectivity, Ericsson Review No. 3, 1998.
8. Arduino UNO Website: http://arduino.cc/en/Main/arduinoBoardUno.
9. Alejandro Pirola, "Setup JY-MCU BT BOARD v1.2", 5-sep-2012, Website: http://apirola.wordpress.com/2012/09/05/setup-jy-mcu-bt-board-v1-2/ .
10. ATMEL Corporation, "ATMEGA328-PU Datasheet (PDF) - ATMEL Corporation - 8-bit Microcontroller with 4/8/16/32K Bytes In-System Programmable Flash", Website: http://www.alldatasheet.com/datasheet-pdf/pdf/392284/ATMEL/ATMEGA328-PU.html.
11. Arduino Tutorial on Serial Communication, *www.ladyada.net/learn/arduino/lesson4.html*
12. Rick Smith, "Understanding encryption and cryptography basics", Information Security magazine - January 2003 Website:http://searchsecurity.techtarget.com/Understanding-encryption-and-cryptography-basics .